NETWORK SECURITY TESTING

DATA SHEET

What is a Network Security Assessment / Penetration Test?

A penetration test, often referred to as pen testing, is an evaluation of your organization's network security. The purpose of a penetration test is to identify security weaknesses that expose your environment to malicious attacks. Unlike a traditional vulnerability assessment that only identifies security vulnerabilities within the tested environment, a penetration test usually takes it a step further by demonstrating potential impact. Demonstrating a potential impact stemming from the exploitation of a security weakness allows an organization to determine the severity of the exploited security vulnerability.

Over a number of years performing penetration testing engagements, we understand the needs and expectations of customers who demand high quality, valuable, and comprehensive information security services. Performing a penetration test allows your organization to perform an assessment on more than just the security vulnerabilities present within the environment.

By performing a penetration test, your organization can gain an understanding of:

- Security vulnerabilities present within the environment
- Incident response procedures, including monitoring and alerting
- Potential impact of a security breach
- Effectiveness of implemented technical and compensating controls

We offer two different penetration testing services to guide your organization to a better security posture and program. Below are information pertaining to our most commonly requested penetration testing services:

INTERNAL NETWORK PENETRATION TESTING

Using a device connected to your internal environment, our consultants will discover security vulnerabilities present within the internal network environment. These activities simulate that of a malicious attacker.

EXTERNAL NETWORK PENETRATION TESTING

Assuming the role of a malicious attacker from the public Internet, our consultants will identify security flaws within your external network environment. These flaws can include patching, configuration, and authentication issues.

carmichael
consulting solutions

Our Penetration Testing Methodology

Based on our professional experience, research, and the activities performed by modern-day attackers, our consultants follow a penetration testing methodology that combines both traditional and new attack techniques to provide quality penetration testing services.

INTELLIGENCE GATHERING

Information about your organization is gathered to map out the environment. In the case of an external penetration test, information such as domains, IP addresses and ranges, compromised email addresses, and employee information is discovered.

VULNERABILITY ANALYSIS

Once the targets have been identified, our certified consultant uses both automated and manual vulnerability analysis tools to identify security flaws.

POST-EXPLOITATION

Demonstration of impact is performed by attempting to escalate access into systems and/or sensitive data within the environment.

THREAT MODELING

An assessment of the organization's business is performed, which includes identifying the most critical business resources. From this analysis, the consultant identifies the best approach to formulating an attack against the exposed security flaws.

PERFORM EXPLOITATION

Depending on the security flaws exposed, exploitation is performed to attempt gaining unauthorized access to systems and/or sensitive data.

TIMELY REPORTING

Documentation is collected, reviewed, and presented to your organization in a clear, concise, and effective manner. In addition to supporting data, strategic and technical recommendations are provided to help your organization with successful remediation.